EXTION

A Project Report On

Network Vulnerability Assessment

Submitted in Fulfilment for the Task 1 of

Cyber security Internship

At

Extion Infotech

Submitted by

Hetvi D. Mehta

Table of Contents

Chapter 1 : Introduction

Network vulnerability assessments are critical for identifying weaknesses that could be exploited by attackers, thereby ensuring the security and resilience of an organization's infrastructure. Tools like Nessus play an essential role in modern cybersecurity by offering comprehensive scanning capabilities to detect and mitigate potential threats effectively.

Objective

To identify and analyze at least five critical vulnerabilities within the network, assess their impact, and propose effective mitigation strategies to enhance security. The objective includes delivering measurable outcomes such as improved CVSS scores and minimized exploitation risks. identify and analyze network vulnerabilities using Nessus and propose effective mitigation strategies to enhance the network's security posture.

Background

Network vulnerabilities can lead to unauthorized access, data breaches, and denial of service attacks. Nessus is a powerful tool used globally for vulnerability assessment. It scans systems, identifies weaknesses, and provides actionable insights to address security risks.

Chapter 2 : Nessus Overview

1. Nessus Introduction

1.1 Overview of Nessus

Nessus is a highly trusted and widely used vulnerability scanning tool developed by Tenable, Inc., designed to identify and mitigate security vulnerabilities across systems, networks, and applications. It is a critical tool in the cybersecurity toolkit, helping organizations proactively identify weaknesses before they can be exploited by attackers.

Initially released in 1998 as an open-source project, Nessus has since grown into a robust commercial product that is trusted by over 30,000 organizations globally. The tool's evolution reflects its adaptability to the ever-changing cybersecurity landscape, making it an indispensable asset for security professionals aiming to protect sensitive data and critical infrastructure.

By providing comprehensive scanning, actionable insights, and integration capabilities, Nessus empowers organizations to fortify their defenses, reduce risks, and ensure compliance with industry standards and regulations.

2. Key Features

2.1 Vulnerability Scanning

Nessus excels at conducting thorough vulnerability assessments by scanning systems and networks for known weaknesses. Using an extensive database of over **100,000 threat signatures**, Nessus detects vulnerabilities in operating systems, applications, databases, and devices. These scans identify issues such as:

- **Misconfigurations** (e.g., weak passwords, incorrect permissions).
- **Outdated software** with known vulnerabilities.
- **Unsecured services** exposed to external threats.
  This level of detail ensures that organizations can address potential issues effectively.

2.2 Extensive Plugin Library

Nessus leverages a vast library of plugins, with new ones added regularly to address emerging threats. Each plugin is designed to detect specific vulnerabilities, compliance issues, or configuration errors.

- Plugins are categorized by functionality, including those targeting operating systems, network devices, and specific compliance standards.

- Nessus's plugin system enables organizations to stay ahead of the latest threats by dynamically updating their scanning capabilities.

2.3 Customizable Scan Policies

Nessus allows users to create tailored scan policies that align with their unique security requirements. This flexibility includes:

- Defining scan scopes and selecting specific targets or groups of devices.
- Focusing on compliance standards like PCI DSS, HIPAA, or ISO 27001.
- Excluding unnecessary scans to optimize performance and reduce resource consumption.
  Customizable policies ensure that scans are efficient and focused on the organization's most critical assets.

2.4 Detailed Reporting

Nessus generates detailed, actionable reports that enable organizations to understand and prioritize vulnerabilities effectively. Key features include:

- **Severity ratings**: Categorizing vulnerabilities as critical, high, medium, or low based on their potential impact.
- **Remediation steps**: Clear and actionable recommendations for addressing each identified issue.
- **Executive summaries**: High-level overviews for stakeholders who need insights without technical jargon.
  The reporting feature is invaluable for ensuring accountability and communicating findings across teams.

2.5 Integration and Automation

Nessus supports seamless integration with other security tools, such as SIEM (Security Information and Event Management) platforms, IT ticketing systems, and threat intelligence feeds.

- The Nessus API enables automation of routine tasks, such as scheduling scans, extracting data, and integrating results into custom dashboards.
- This integration reduces manual workloads and enables organizations to create efficient, streamlined workflows that improve response times.

2.6 User-Friendly Interface

One of Nessus's standout features is its intuitive, web-based interface, which simplifies complex tasks such as configuring scans, analyzing results, and generating reports.

- Designed for ease of use, the interface caters to both novice users and seasoned security professionals.
- Features such as preconfigured templates and guided workflows enable quick setup and effective results.
  This ease of use makes Nessus a go-to solution for organizations of all sizes and technical expertise levels.

3. Advantages of Nessus

3.1 Comprehensive Detection

Nessus provides exhaustive vulnerability detection, covering a wide range of issues, including:

- **Operating system vulnerabilities** across Linux, Windows, and macOS.
- **Application vulnerabilities**, including web applications and databases.
- **Network device vulnerabilities**, such as firewalls, routers, and IoT devices.
  By offering broad coverage, Nessus ensures no critical vulnerabilities go unnoticed.

3.2 Ease of Use

Nessus is designed to be user-friendly, requiring minimal training to operate effectively. With features like preconfigured policies and templates, users can quickly initiate scans and interpret results. Its straightforward setup makes it accessible to small businesses and large enterprises alike.

3.3 Customizability

Organizations can tailor Nessus to their specific needs by:

- Adjusting scan settings to focus on critical assets.
- Creating policies for compliance with specific regulatory requirements.
- Scheduling automated scans during non-peak hours to minimize disruptions.
  This level of customization makes Nessus a flexible solution for varying security demands.

3.4 Cost-Effectiveness

Compared to other enterprise-grade vulnerability management solutions, Nessus provides excellent value for its price. It offers powerful features at a fraction of the cost of competitors, making it ideal for organizations seeking comprehensive security on a budget.

3.5 Regular Updates

Nessus continuously updates its plugins and vulnerability database to address the latest threats.

- These updates occur frequently and are automated, ensuring the tool remains effective against emerging vulnerabilities without manual intervention.

3.6 Integration Capabilities

Nessus's ability to integrate with SIEM platforms, ticketing systems, and other security tools enhances its utility within an organization's broader security ecosystem.

- Integration ensures that vulnerability data is not siloed but contributes to overall security operations and incident response processes.

4. Nessus Setup

4.1 Download and Installation

To begin using Nessus, download and install it on your desired platform:

- **Download**: Visit the official Tenable website and select the appropriate Nessus version for your operating system (Windows, Linux, or macOS).
- **Installation**: Follow platform-specific instructions provided by Tenable to install Nessus. These include steps for installing dependencies, executing installation scripts, and verifying successful installation.
- **Choose Edition**: Depending on your needs, select the appropriate edition (e.g., Nessus Essentials for free vulnerability scanning, Nessus Professional for in-depth vulnerability management, or Tenable.io for cloud-based operations).

4.2 Initial Configuration

After installation, complete the initial setup:

- **Access the Web Interface**: Launch a browser and navigate to https://localhost:8834 or the server's IP address.
- **Administrator Account**: Create an admin account by setting up a username, password, and email.
- **License Activation**: Enter the Nessus activation code or license key to unlock features.
- **Network Configuration**: Specify proxy settings or firewall rules, if needed, for external communication.

4.3 Plugin Updates

Plugins are integral to Nessus's ability to detect vulnerabilities.

- **Initial Update**: Perform a plugin database update immediately after installation to include the latest threat signatures.
- **Automatic Updates**: Configure automatic plugin updates in Nessus settings to ensure the tool is always prepared for emerging threats.
- **Validation**: Confirm successful updates via the dashboard, which shows the plugin version and update history.

5. Configuration

5.1 Policy Creation

Scan policies define how Nessus conducts vulnerability scans:

- **Select Scan Type**: Choose from several scan types, such as:
    - **Basic Network Scan**: Identifies vulnerabilities in general network environments.
    - **Web Application Scan**: Focuses on web-specific vulnerabilities like SQL injection or cross-site scripting (XSS).
    - **Compliance Scan**: Ensures systems adhere to regulatory standards such as PCI DSS or HIPAA.
- **Plugin Selection**: Enable or disable specific plugins to customize the focus of the scan based on organizational requirements.
- **Custom Policies**: Save and reuse policies tailored to specific needs, such as scanning only critical systems or testing new configurations.

5.2 Target Definition

Clearly define the scope of scans to improve efficiency and avoid unnecessary resource consumption:

- **Specify Targets**: Add IP addresses, hostnames, or IP ranges to include in scans.
- **Asset Grouping**: Organize targets into groups based on location, department, or criticality.
- **Exclusions**: Define IP addresses or ranges to exclude from scans, preventing disruptions to sensitive systems.

5.3 Advanced Options

Leverage advanced configurations for more precise and efficient scans:

- **Authentication**: Use administrative credentials to enable authenticated scans, uncovering deeper vulnerabilities that may not be visible otherwise.
- **Schedule Scans**: Automate scan execution during off-peak hours or at regular intervals to ensure continuous monitoring without disrupting operations.
- **Performance Tuning**: Adjust scan settings, such as parallel scan limits or timeout thresholds, to align with network and system capacity.

6. Vulnerability Identification

6.1 CVSS-Based Categorization

Nessus ranks vulnerabilities using the **Common Vulnerability Scoring System (CVSS)** to help organizations prioritize remediation efforts:

- **Critical (CVSS 9.0–10.0)**:
    - Easily exploitable vulnerabilities with severe consequences, such as system takeovers or data breaches.
    - Require immediate remediation.
- **High (CVSS 7.0–8.9)**:
    - Serious vulnerabilities with a high probability of exploitation.
    - Could lead to significant damage if not addressed promptly.
- **Medium (CVSS 4.0–6.9)**:
    - Moderate vulnerabilities that require specific conditions for exploitation.
    - Address these vulnerabilities within a reasonable timeframe.
- **Low (CVSS 0.1–3.9)**:
    - Minor issues that pose limited risk.
    - Often addressed as part of routine maintenance.
- **Informational**:
    - System details and configuration findings that don’t represent vulnerabilities but provide insights for improving security posture.

6.2 Vulnerability Insights

Nessus provides detailed insights into each identified vulnerability to guide remediation efforts:

- **Severity**: Assigns a CVSS-based severity level to highlight the urgency of each issue.
- **Description**: Explains the nature of the vulnerability, including its cause and potential impact.
- **Impact Analysis**: Details risks associated with exploitation, such as data loss, service disruption, or unauthorized access.
- **Remediation Recommendations**: Offers actionable guidance, such as applying software patches, adjusting configurations, or isolating affected systems.
- **References**: Links to external sources, such as CVE databases or vendor advisories, for additional context and verification.

6.3 Vulnerability Management Workflow

To effectively manage identified vulnerabilities:

1. **Scan Results Review**: Analyze scan reports to understand the distribution of vulnerabilities by severity and affected assets.
2. **Prioritize Issues**: Focus on resolving critical and high-severity vulnerabilities first.
3. **Remediate**: Implement the recommended fixes for each issue, including applying patches or modifying configurations.
4. **Rescan**: Verify that vulnerabilities have been resolved by performing a follow-up scan.

Chapter 3 : Nessus Vulnerability Scan Report

Metasploit

Report generated by Tenable Nessus™ Fri, 24 Jan 2025 23:52:41 India Standard Time

Vulnerabilities by Host

TABLE OF CONTENTS

Vulnerabilities by Host

192.168.253.130

8	6	20	8	76
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 118

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	0.974	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0*	5.1	0.1994	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.1994	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	7.4	0.6956	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0053	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	0.0398	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0489	90509	Samba Badlock Vulnerability
HIGH	7.5*	7.4	0.015	10205	rlogin Service Detection
HIGH	7.5*	7.4	0.015	10245	rsh Service Detection
MEDIUM	6.8	6.0	0.2471	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisonir
MEDIUM	6.5	4.4	0.004	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate

MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	4.4	0.9726	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.003	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	3.6	0.935	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolet and Weakened eNcryption)
MEDIUM	5.9	4.4	0.0079	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	-	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.3	4.0	0.0225	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	57608	SMB Signing not required
MEDIUM	5.3	-	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	7.3	0.0135	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	0.9488	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FRE
LOW	3.7	6.5	0.498	70658	SSH Server CBC Mode Ciphers Enabled
LOW	3.7	-	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	4.5	0.9689	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
LOW	3.7	4.5	0.9689	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Support (Logjam)
LOW	3.4	5.1	0.9744	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	2.2	0.8939	10114	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	-	10407	X Server Detection

INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	21186	AJP Connector Detection
INFO	N/A	-	-	18261	Apache Banner Linux Distribution Disclosure
INFO	N/A	-	-	48204	Apache HTTP Server Version
INFO	N/A	-	-	39446	Apache Tomcat Detection
INFO	N/A	-	-	84574	Backported Security Patch Detection (PHP)
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)
INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10028	DNS Server BIND version Directive Remote Version Detection
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	72779	DNS Server Version Detection
INFO	N/A	-	-	35371	DNS Server hostname.bind Map Hostname Disclosure
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	35716	Ethernet Card Manufacturer Detection
INFO	N/A	-	-	86420	Ethernet MAC Addresses
INFO	N/A	-	-	10092	FTP Server Detection
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11156	IRC Daemon Version Detection
INFO	N/A	-	-	10397	Microsoft Windows SMB LanMan Pipe Server Listing Disclosur
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)

INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remo check)
INFO	N/A	-	-	10437	NFS Share Export List
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	181418	OpenSSH Detection
INFO	N/A	-	-	50845	OpenSSL Detection
INFO	N/A	-	-	48243	PHP Version Detection
INFO	N/A	-	-	66334	Patch Report
INFO	N/A	-	-	118224	PostgreSQL STARTTLS Support
INFO	N/A	-	-	26024	PostgreSQL Server Detection
INFO	N/A	-	-	22227	RMI Registry Detection
INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	10263	SMTP Server Detection
INFO	N/A	-	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	153588	SSH SHA-1 HMAC Algorithms Enabled
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	-	10863	SSL Certificate Information

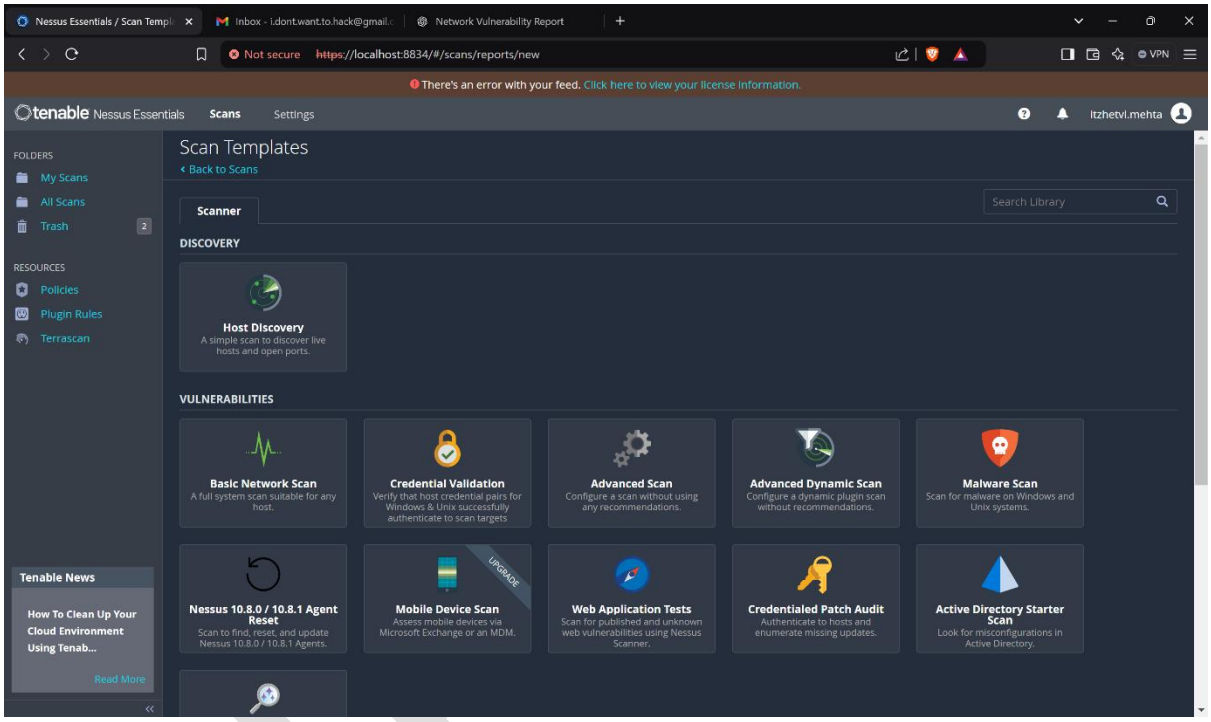
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	62563	SSL Compression Methods Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	51891	SSL Session Resume Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	25240	Samba Server Detection
INFO	N/A	-	-	104887	Samba Version
INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	17975	Service Detection (GET request)
INFO	N/A	-	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	-	11819	TFTP Daemon Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	10281	Telnet Server Detection
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	-	-	20094	VMware Virtual Machine Detection
INFO	N/A	-	-	19288	VNC Server Security Type Detection
INFO	N/A	-	-	65792	VNC Server Unencrypted Communication Detection
INFO	N/A	-	-	10342	VNC Software Detection
INFO	N/A	-	-	135860	WMI Not Available
INFO	N/A	-	-	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	-	-	11422	Web Server Unconfigured - Default Install Page Present

INFO	N/A	-	-	11424	WebDAV Detection
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	-	-	52703	vsftpd Detection

* indicates the v3.0 score was not available; the v2.0 score is shown

Chapter 4 : Critical Vulnerabilities and its Mitigation Plan

When performed advanced scan on the target, Total of 118 vulnerabilities found in which 76 Informational, 8 Low, 20 Medium, 6 High and 8 Critical Vulnerabilities.



1. Apache Tomcat AJP Connector Request Injection (Ghostcat)

- **Description:** Ghostcat (CVE-2020-1938) is a vulnerability in Apache Tomcat's AJP Connector that allows attackers to read arbitrary files on the server and potentially execute remote code.
- **Impact:** Remote code execution or exposure of sensitive files.
- **Mitigation Steps:**
    1. **Upgrade:** Update Apache Tomcat to the latest version where the issue is resolved.
    2. **Restrict Access:** Disable the AJP Connector if not required or configure it to listen only on trusted IPs.
    3. **Secure Configuration:** Add authentication for AJP connections if needed.

2. Bind Shell Backdoor Detection

- **Description:** The system is detected with a backdoor that allows unauthorized remote access via a shell.
- **Impact:** Attackers can gain remote control, bypassing authentication.
- **Mitigation Steps:**
    1. **Remove Malicious Shell:** Locate and remove the backdoor binary or script.
    2. **Update Antivirus/IDS:** Use updated intrusion detection systems to scan for malicious activity.
    3. **Secure Access:** Implement firewalls to block unauthorized access to exposed ports.

3. SSL Version 2 and 3 Protocol Detection

- **Description:** SSL v2 and v3 are outdated encryption protocols vulnerable to attacks such as POODLE and BEAST.
- **Impact:** Exposure to protocol-based attacks, leading to data interception.
- **Mitigation Steps:**
    1. **Disable SSL v2/v3:** Configure servers to use only modern TLS versions (1.2 or 1.3).
    2. **Update Software:** Ensure all services using SSL/TLS are updated to the latest secure versions.
    3. **Reconfigure Cipher Suites:** Use strong ciphers and remove weak or deprecated ones.

4. Apache Tomcat SEoL (<= 5.5.x)

- **Description:** End-of-life versions of Apache Tomcat are vulnerable to various unpatched exploits.
- **Impact:** Exploitation of unpatched vulnerabilities leading to compromise.
- **Mitigation Steps:**
    1. **Upgrade:** Update to the latest supported version of Apache Tomcat.
    2. **Secure Environment:** Configure strong security policies, including firewalls and access controls.

5. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

- **Description:** A flaw in the Debian OpenSSL package (CVE-2008-0166) resulted in weak cryptographic keys, making encrypted data vulnerable.
- **Impact:** Predictable encryption keys compromise data confidentiality.
- **Mitigation Steps:**
    1. **Update:** Install the patched versions of OpenSSH and OpenSSL.
    2. **Regenerate Keys:** Replace all cryptographic keys generated using the vulnerable package.
    3. **Audit Systems:** Identify and replace affected keys across the environment.

6. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL Check)

- **Description:** Similar to the above, this specific detection highlights SSL key weaknesses due to the same flaw.
- **Impact:** Weak SSL encryption compromises secure communications.
- **Mitigation Steps:**
    1. **Patch OpenSSL:** Update OpenSSL to the fixed version.
    2. **Regenerate Certificates:** Reissue all SSL/TLS certificates.
    3. **Audit Dependencies:** Review services and libraries relying on the vulnerable versions.

7. UnrealIRCd Backdoor Detection

- **Description:** A backdoored version of UnrealIRCd allows remote command execution.
- **Impact:** Complete system compromise via remote execution.
- **Mitigation Steps:**
    1. **Verify Software Source:** Reinstall UnrealIRCd using a verified, clean version.
    2. **Audit Files:** Ensure no malicious scripts or binaries remain.
    3. **Implement Monitoring:** Deploy security tools to detect future unauthorized changes.

8. VNC Server 'password' Password

- **Description:** VNC servers configured with a weak or default password ("password") are susceptible to unauthorized access.
- **Impact:** Attackers can gain remote control over the system.
- **Mitigation Steps:**
    1. **Change Default Password:** Immediately update the VNC password to a strong, complex one.
    2. **Enable Authentication:** Use multi-factor authentication where possible.
    3. **Restrict Access:** Configure firewalls to allow VNC connections only from trusted IPs.

Chapter 5 : Conclusion

This report highlights several critical vulnerabilities within the organization's network infrastructure, including issues such as outdated software, insecure configurations, and the presence of malicious backdoors. Each identified vulnerability presents significant risks, including data breaches, unauthorized access, and system compromise.

To mitigate these risks, immediate action is necessary. This includes updating outdated software, disabling deprecated protocols, strengthening authentication mechanisms, and implementing robust monitoring systems. The outlined mitigation strategies aim to ensure not only the resolution of current vulnerabilities but also the establishment of a more secure network environment for the future.

Organizations must adopt a proactive approach to cybersecurity, emphasizing regular vulnerability assessments, continuous monitoring, and adherence to industry best practices. By doing so, the organization can safeguard its critical assets, maintain operational integrity, and foster trust among stakeholders.